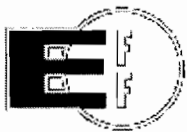


Exhibit 5

[About EFF](#)[Cases](#)[Press Room](#)[DeepLinks](#)[Action Center](#)[Join EFF](#)[Sitemap](#) | [Calendar](#)

Search DeepLinks

Deep Links

NOTEWORTHY NEWS FROM AROUND THE INTERNET

« [Report from Hearing on National Security Letters](#) | [Main](#) | [DMCA](#)
Used to Stymie Competition...Again »

Uproot Sony-BMG's Invasion of Your Privacy and Your Computer

November 03, 2005

For years now, copy-restriction software has been a looming threat to those who purchase music and want to make fair uses such as space-shifting it from one device or computer to another. Fortunately, early versions of the software were so cumbersome and easy to work around that consumers whole-heartedly rejected or bypassed them. Recently, however, at least one record label has stepped up the war for control of digital content by drawing from the playbook of spyware companies and virus-writers.

Using a program called a rootkit, inserting a Sony BMG music CD will now infect your computer with a nefarious program, burying it deeply and obscurely within your operating system. The program will monitor your computer activity in the name of preventing the so-called epidemic of "piracy" that results from people making extra copies of their music CDs or favorite songs. Worse yet, there is no "uninstall" feature on this program. It's like the roach motel -- once Sony BMG's surveillance program checks in, you can't make it check out without completely wiping your entire system clean. Such practices have been widely condemned in the computer world, even by Microsoft's own research division.

Outrage from computer users and music fans has sparked Sony BMG into offering a program on its website that will show you if you have been infected with the rootkit. However, while you can see the program running, you still can't uninstall it, and some security experts believe installing the "update" may even infect your computer with more unwanted files.

While it is debatable whether copy-restriction software can even prevent serious illegal copying to begin with, there should be no question that invading our computers and infecting our systems should be off-limits. Unfortunately, the law is unclear on the exact rights users have to keep programs like Sony's rootkit off your computer when you purchase their CDs or click on a random "I Agree" button that might appear during an installation process. Until the law clarifies that We the Consumer actually hold the rights and keys to our computers, spyware companies, virus-makers, and now even entertainment conglomerates will be the

Search [eff.org](#)

Enter search terms

Powered by
Google

Search EFF

» [About EFF's search](#)

[Contents](#)[miniLinks](#)[Awards](#)[EFF Victories](#)[EFF White Papers](#)[EFFector](#)

**Subscribe to
EFFector!**

[our free email
newsletter]

Email:

 Zip / Postal Code
(optional)

» [EFFector Archive](#)

[Topics](#)[Anonymity](#)[Biometrics](#)[Bloggers' Rights](#)[Broadcast Flag](#)[CALEA](#)[CAPPS II](#)[Censorship](#)[Copyright Law](#)[Digital Rights](#)[Management \(DRM\)](#)[DMCA](#)[Domain names](#)[E-voting](#)[File-sharing](#)[Filtering](#)[FTAA](#)[Intellectual Property](#)[International](#)

Archives

[March 2006](#)[February 2006](#)[January 2006](#)[December 2005](#)[November 2005](#)[October 2005](#)[September 2005](#)[August 2005](#)[July 2005](#)[June 2005](#)[May 2005](#)[April 2005](#)[March 2005](#)[February 2005](#)[January 2005](#)[December 2004](#)[November 2004](#)[October 2004](#)[September 2004](#)[August 2004](#)[July 2004](#)[June 2004](#)[May 2004](#)[April 2004](#)[March 2004](#)

DeepLinks Topics

[Announcements](#)[CALEA](#)[Cell Tracking](#)[Digital Television](#)[DRM](#)[E-voting](#)

[E-voting Lobby Days](#)
[EFF15](#)
[File sharing](#)
[Free Speech](#)
[Intellectual Property](#)
[Misc.](#)
[Patents](#)
[Privacy](#)
[Standards/Architecture](#)
[Trusted Computing](#)
[USA PATRIOT](#)
[WIPO](#)

Get Email

Enter your email address to get posts by email:

Submit

RSS Feeds

[RSS 1.0](#)
[RSS 2.0](#)

ones dictating what we can and cannot do in the privacy of our own homes with the equipment and content we have lawfully purchased. Left unchecked, they will continue using our own computers against us to enforce their will and whims over our personal freedoms and behavior.

Entertainment companies often complain that computer users refuse to respect their intellectual property rights. Yet tools like Sony's rootkit refuse to respect our own personal property and privacy rights. Such hypocrisy should not stand.

Note: According to Princeton University CS Prof. Ed Felten, if you're using a recent version of Windows, you can protect yourself against this type of software, and some other security risks, by disabling autorun.

UPDATE: Calling the rootkit a "security risk," Symantec has just released a [new removal tool](#) that targets the risk. Professor Ed Felten has also posted a [Sony DRM Customer Survival Kit](#) with tools for figuring out whether you've been infected with the rootkit, how to disable it, how to disable the DRM software altogether, etc.

[Internet governance](#)
[ISP legalities](#)
[Licensing/UCITA](#)
[Linking](#)
[Patents](#)
[Pending legislation](#)
[Privacy](#)
[Public records/FOIA](#)
[Reverse engineering](#)
[RFID](#)
[Spam](#)
[States](#)
[Surveillance](#)
[USA PATRIOT Act](#)
[Wireless](#)
[WIPO](#)
[EFF en Español](#)
[Recursos e información de EFF en Español.](#)

Posted by Jason Schultz at 10:01 AM | [Permalink](#) | [Technorati](#)

[Home](#) | [About EFF](#) | [Cases](#) | [Press Room](#) | [DeepLinks](#) | [Action Center](#) | [Join EFF](#) | [Privacy Policy](#) | [EFF RSS Feeds](#)